So What?
How Cigital Approaches Risk Management

Software Confidence. Achieved.

Jeffery Payne
Chief Executive Officer
Cigital, Inc.

jepayn@cigital.com

www.cigital.com
info@cigital.com
703 404 9293

December 2005

cigital

About Cigital

- Cigital helps organizations improve the quality and security of their software applications
- Focused on software assurance since 1992
- Cigital Labs – cutting edge software quality research laboratory

Risk Management is the Cornerstone of our Business

- Why?
  - RM provides our quality assurance/IV&V methodology a means of assuring systems of differing levels of criticality
  - RM drives selection of validation techniques and associated exit criteria based upon risk and consequence of failure
  - Risk is a great metric to track for both delivery and sales!
  - Answers the ‘So What’ question

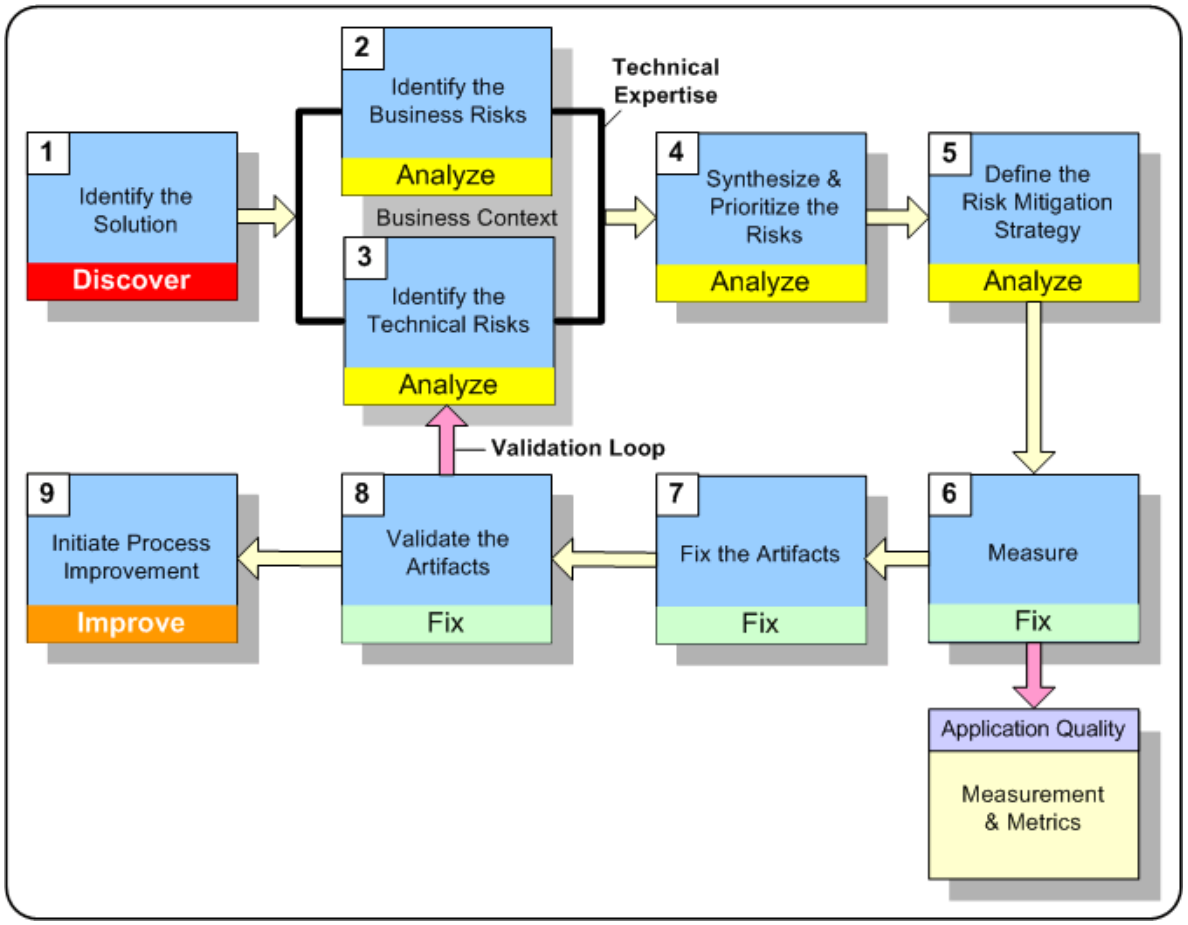
cigital

So What?

- Identifying defects, flaws, issues, vulnerabilities, bugs, untestable features, missing requirements, potential problems, poor process, poor management, etc. is often not enough to spark **action** on the development side of the house.
- Need to tie issues to a consequence of failure to demonstrate **why** such issues must be addresssed.
- Why?
  - Developers only want to fix what needs to be fixed
  - Budgets are always tight
  - Business executives only care about items that impact the bottom line
  - Sarbanes-Oxley says so ;-)

cigital

Our Risk Management Approach for Software



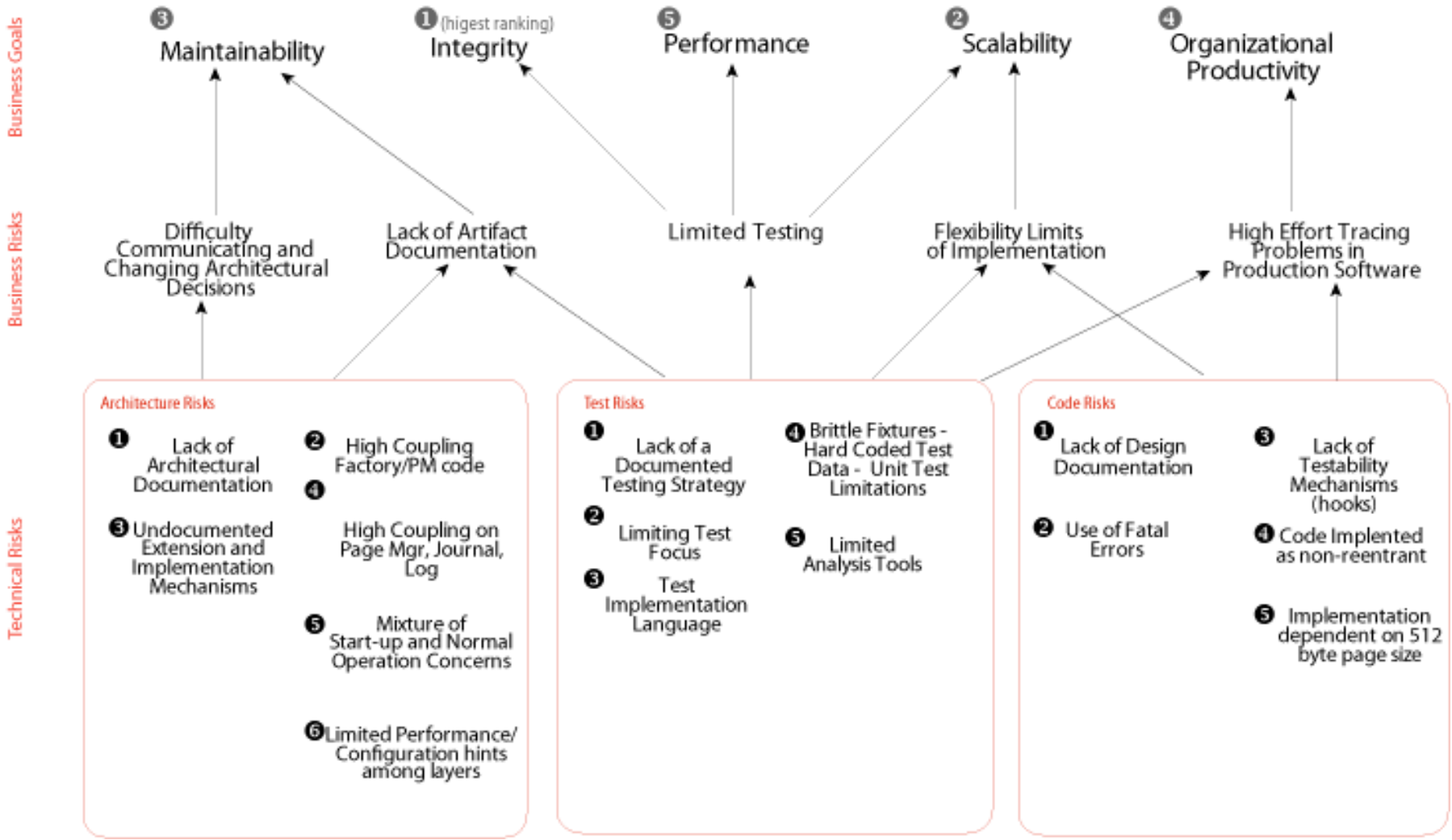
cigital

Keys to Software Risk Management

- *Go Deep* – Identify deep technical risks in the artifacts
- *Categorize* – Relate risks together so as not to overwhelm your customer
- *Answer So What* - Tie to business consequence and goals
- *Demonstrate* – Show a key vulnerability for effect
- *Help Improve* – Create a roadmap that incrementally reduces risk and improves the product

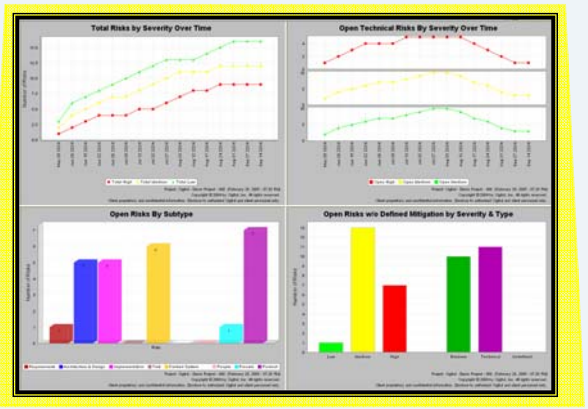
cigital

Goals to Risks Mapping



cigital

The Cigital Workbench™



Measurement and Metrics

SDLC Activities | Artifact Quality | Process Improvement | ... | Risk Mitigation

Best Practices → Knowledge → Process

Control
Risk Management

Manageability
Dashboard
- Risk
- Artifact quality & security
- Process metrics

Predictability
Processes & analysis rules

Insight & Understanding
Knowledge & Expertise

Thank you for your time

Software Confidence. Achieved.